

# ELEMENTS WITH $r$ -TH ROOTS IN FINITE GROUPS

E. KHAMSEH, M. R. R. MOGHADDAM, F. G. RUSSO, AND F. SAEEDI

ABSTRACT. The probability that a randomly chosen element of a finite group is an  $r$ -th root (for any integer  $r \geq 2$ ) has been studied largely in case  $r = 2$ . Certain techniques may be generalized for  $r > 2$  and here we find the exact value of this probability for projective special linear groups. A result of density is placed at the end, in order to show an analogy with the case  $r = 2$ .

## 1. INTRODUCTION

In the present paper all the groups are finite. In a group  $G$ , if there exists an element  $y \in G$  for which  $x = y^r$ , we say that  $x$  has an  $r$ -th root. For  $r = 2$ , J. Blum described in [1] the probability

$$\text{Prob}_2(S_n) = \frac{|S_n^2|}{n!}$$

that a randomly chosen permutation of length  $n$  has a 2-nd root (or square root), where  $S_n$  is the permutation group on  $n$  letters. Successively his work was generalized in [3, 5, 6, 8] to the case of an arbitrary group. Already in [2, 7] it was studied the probability

$$\text{Prob}_r(S_n) = \frac{|S_n^r|}{n!}$$

that a randomly chosen permutation of length  $n$  has an  $r$ -th root for  $r \geq 2$ . Therefore, many results in [1] can be found as special situations of [2, 7], but, so far as we have searched in the literature, [2, 7] have not been extended in the sense of [3, 5, 6, 8] to the case of an arbitrary group. This is the beginning of our investigations and the motivation of the present work. We define the probability

$$\text{Prob}_r(G) = \frac{|G^r|}{|G|},$$

where  $r \geq 2$  and  $G^r = \{g^r \mid g \in G\}$  is the set of all elements of  $G$  having at least one  $r$ -th root. Unfortunately,  $G^r$  is not a subgroup of  $G$  but only a set and this can give difficulties from the general point of view.

Even if  $\text{Prob}_2(G)$  is known by [3, 5, 6] and  $\text{Prob}_r(S_n)$  by [2, 7], we have not found whether it is possible to obtain some structural information on  $G$  from the bounds of  $\text{Prob}_r(G)$  or not. In the present paper we will investigate such aspects and provide some restrictions of numerical nature for  $\text{Prob}_r(G)$ .

---

2010 *Mathematics Subject Classification.* Primary 20D15; 20P05; Secondary 20D60.

*Key words and phrases.*  $r$ -th roots, probability, equations over finite groups, linear groups.

## 2. BASIC PROPERTIES

We recall some fundamental notions on abelian groups. If  $A$  is an abelian group, then

$$A^r = \{a^r \mid a \in A\}$$

is a subgroup of  $A$  and  $A$  is called  $r$ -divisible, if  $A^r = A$ .  $A$  is *divisible*, if it is  $r$ -divisible for all  $r \geq 2$ . It is easy to see that  $A$  is divisible if, and only if, it is  $p$ -divisible for all primes  $p$ .

$$A[r] = \{a \in A \mid a^r = 1\}$$

is a subgroup of  $A$  and  $A$  is of *exponent*  $r$ , if  $A[r] = A$ . If  $r = p$  is a prime,  $A[p]$  is called  $p$ -*socle* of  $A$  and is isomorphic to the additive group of a vector space over the field with  $p$  elements: In other words,  $A[p]$  is an elementary  $p$ -group of rank  $k \geq 1$ , that is,

$$A[p] = C_p \times \dots \times C_p = C_p^k.$$

In general, for an arbitrary  $r \geq 2$ , the subgroups  $A^r$  and  $A[r]$  are related by the First Isomorphism's Theorem:  $\varphi : a \in A \mapsto a^r \in A^r$  is a homomorphism of groups, inducing  $A^r \simeq A/A[r]$ . The following remark gives a complete characterization for abelian groups.

**Remark 2.1.** Assume that  $G$  is a nontrivial abelian group.

- (i)  $\text{Prob}_r(G) = \frac{1}{|G[r]|}$ .
- (ii) If  $r$  is prime, then  $\text{Prob}_r(G) = \frac{1}{r^k}$  for some  $k \geq 1$ . Furthermore, the set

$$X = \{\text{Prob}_r(G) \mid G \text{ is an abelian group}\}$$

coincides with the subset

$$Y = \left\{ \frac{1}{r^k} \mid k \geq 1 \right\}$$

of the interval  $[0, 1]$ .

From Remark 2.1 (i), a nontrivial abelian group  $G$  of exponent  $r$  has  $\text{Prob}_r(G) = \frac{1}{|G|}$ . Now we will summarize most of the above considerations in the next result.

**Proposition 2.2.** *Let  $G$  be a nontrivial abelian group.*

- (i)  $\text{Prob}_r(G) = \frac{1}{|G[r]|}$ . Furthermore, if  $r$  is prime,  $\text{Prob}_r(G) = \frac{1}{|G|}$  if and only if  $G \simeq C_r^k$  for some  $k \geq 1$ .
- (ii) The sets  $X$  and  $Y$  of Remark 2.1 coincide.

*Proof.* (i). The first part is exactly Remark 2.1 (i). Now assume that  $r$  is prime. If  $G \simeq C_r^k$ , then  $G$  is isomorphic to the additive group of a vector space over the field with  $p$  elements, that is,  $G[r] \simeq G$ . Then  $\text{Prob}_r(G) = \frac{1}{|G|}$ . Conversely,  $\text{Prob}_r(G) = \frac{|rG|}{|G|} = \frac{|G|}{|G[r]| |G|} = \frac{1}{|G[r]|} = \frac{1}{|G|}$  implies  $|G[r]| = |G|$ , then  $1 = |rG| = \frac{|G|}{|G[r]|}$  via the isomorphism induced by  $\varphi$ , and so  $G[r] \simeq G$ , from which the result follows.

(ii). It is exactly Remark 2.1 (ii).  $\square$

Now we describe  $\text{Prob}_r(G) = 1$  for  $r \geq 2$  and recall notions in [5, 6].

**Remark 2.3.** Let  $G$  be a nontrivial group.

- (i)  $\text{Prob}_r(G) = 1$  if and only if  $|G| = |G^r|$ , that is, the number of the elements of  $G$  having an  $r$ -th root is the same of the number of the elements of  $G$ .

- (ii) (See [6]) The number of solutions of the equation  $x^r = a$  in  $G$  is a multiple of  $\gcd(r, |C_G(a)|)$ , where  $r \geq 2$  and  $a, x \in G$ . In particular, the number of solutions of the equation  $x^r = 1$  over  $G$  is a multiple of  $\gcd(r, |G|)$  and when  $r$  is prime,  $|x| = |a|$  or  $|x| = r|a|$ .

We reformulate Remark 2.3 as follows.

**Proposition 2.4.** *Let  $G$  be an arbitrary group and  $r \geq 2$ .  $\text{Prob}_r(G) = 1$  if and only if some multiple of  $\gcd(r, |G|)$  is equal to 1.*

Propositions 2.2 and 2.4 agree with [5, Proposition 2.1], when  $r = 2$ . Now we will proceed to list further properties.

**Remark 2.5.** For an arbitrary group  $G$ , we have  $0 < \frac{1}{|G|} \leq \text{Prob}_r(G) \leq 1$ . Propositions 2.2 (i) shows a condition in which we achieve the lower bound  $\frac{1}{|G|}$  in the abelian case. Proposition 2.4 shows a more general condition in which we achieve the upper bound.

It is well-known that the probability of independent events is multiplicative. Here we have as follows.

**Proposition 2.6.** *Given two groups  $A$  and  $B$ ,  $\text{Prob}_r(A \times B) = \text{Prob}_r(A) \text{Prob}_r(B)$ .*

*Proof.*

$$\text{Prob}_r(A \times B) = \frac{|(A \times B)^r|}{|A \times B|} = \frac{|A^r \times B^r|}{|A||B|} = \frac{|A^r||B^r|}{|A||B|} = \text{Prob}_r(A) \text{Prob}_r(B).$$

□

For products of groups we draw the following conclusion.

**Proposition 2.7.** *If  $G = AB$ , where  $A$  and  $B$  are subgroups of  $G$  such that  $[A, B] = 1$ , then*

$$\text{Prob}_r(G) = \frac{1}{|A^r \cap B^r|} \text{Prob}_r(A) \text{Prob}_r(B).$$

*In particular, if  $A \cap B = 1$ , then  $\text{Prob}_r(G) = \text{Prob}_r(A) \text{Prob}_r(B)$ .*

*Proof.* Given  $a \in A$  and  $b \in B$ ,  $(ab)^r = a^r b^r$  if and only if  $[a, b] = 1$ . Therefore  $[A, B] = 1$  implies  $(AB)^r = A^r B^r$  and so  $|A^r B^r| = \frac{|A^r||B^r|}{|A^r \cap B^r|}$ . Then

$$\begin{aligned} \text{Prob}_r(G) &= \frac{|G^r|}{|G|} = \frac{|(AB)^r|}{|AB|} = \frac{|A^r B^r|}{|AB|} = \frac{1}{|A^r \cap B^r|} \frac{|A^r|}{|A|} \frac{|B^r|}{|B|} \\ &= \frac{\text{Prob}_r(A) \text{Prob}_r(B)}{|A^r \cap B^r|}. \end{aligned}$$

In particular,  $A^r \cap B^r \subseteq A \cap B = 1$  implies  $\text{Prob}_r(G) = \text{Prob}_r(A) \text{Prob}_r(B)$ . □

The next two results show bounds in terms of subgroups and quotients.

**Proposition 2.8.** *Let  $N$  be a normal subgroup of a group  $G$ . Then*

$$\text{Prob}_r(G) \leq \text{Prob}_r(G/N).$$

*Proof.* Note that  $gN \in G/N$  has an  $r$ -th root if and only if there is  $xN \in G/N$  for which  $gN = (xN)^r$ , that is,  $x^r \in gN$ . Therefore  $gN \in G/N$  does not have an  $r$ -th root if and only if there is no element  $x \in G$  with  $x^r \in gN$ . Hence, if a coset in  $G/N$  does not have an  $r$ -th root, then no element of this coset has an  $r$ -th root in  $G$ , and therefore  $|G| - |G^r| \geq |N|(|G/N| - |(G/N)^r|)$ . By dividing both sides by  $|G|$  we obtain  $1 - \text{Prob}_r(G) \geq 1 - \text{Prob}_r(G/N)$  and so  $\text{Prob}_r(G) \leq \text{Prob}_r(G/N)$ , as required.  $\square$

**Proposition 2.9.** *Let  $H$  be a subgroup of a group  $G$ . Then*

$$|G|^{-1} \text{Prob}_r(H) \leq \text{Prob}_r(G).$$

*Proof.* Obviously  $H^r \subseteq G^r$  implies  $|H^r| \leq |G^r|$ . Therefore  $\text{Prob}_r(H) \leq |H| \cdot \text{Prob}_r(H) = \frac{|H|}{|H|} \cdot |H^r| \leq \frac{|G|}{|G|} \cdot |G^r| = |G| \cdot \text{Prob}_r(G)$  implies  $|G|^{-1} \text{Prob}_r(H) \leq \text{Prob}_r(G)$  and the lower bound follows.  $\square$

The following result is a lower bound of general interest.

**Corollary 2.10.** *Let  $G$  be a solvable group and  $P$  be a Sylow  $p$ -subgroup of  $G$  for some prime  $p$ . Then  $\frac{1}{|P|} \leq \text{Prob}_p(G)$ .*

*Proof.* Since  $H$  is solvable, there exists a  $p'$ -Hall subgroup  $H$  of  $G$  such that  $|G| = |H||P|$  and  $H = H^p \subseteq G^p$ . Therefore,  $\text{Prob}_p(G) = \frac{|G^p|}{|G|} \geq \frac{|H|}{|G|} = \frac{|H|}{|H||P|} = \frac{1}{|P|}$ .  $\square$

### 3. PROJECTIVE SPECIAL LINEAR GROUPS AND DENSITY

**Theorem 3.1.** *Let  $q$  be a prime power. If  $q \equiv 1 \pmod{4}$ ,  $q$  is odd and  $r = \frac{q-1}{2} \geq 2$  is prime, then*

$$\text{Prob}_r(\text{PSL}(2, q)) = \frac{r+1}{2r}.$$

*In particular, if  $r = 2$ , then  $\text{Prob}_2(\text{PSL}(2, q)) = \frac{3}{4}$ .*

*Proof.* We recall that

$$|\text{PSL}(2, q)| = \frac{q(q-1)(q+1)}{\gcd(2, q-1)} = q(q-1)(q+1).$$

Let  $\nu$  be a generator of the multiplicative group of the field of  $q$  elements. Denote

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 0 \\ \nu & 1 \end{pmatrix}, \quad a = \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix}.$$

and  $b$  an element of order  $q+1$  (Singer cycle) in  $\text{SL}(2, q)$ . By abuse of notation, we use the same symbols for the corresponding elements in  $\text{PSL}(2, q) = \text{SL}(2, q)/Z(\text{SL}(2, q))$ . From the character table of  $\text{SL}(2, q)$  (see [4, Theorem 38.1]), one gets easily the character table of  $\text{PSL}(2, q)$ . We reproduce it below for the convenience of the reader. The elements  $1, c, d, a^l$  and  $b^m$  for  $1 \leq l \leq \frac{q-1}{4}$  and  $1 \leq m \leq \frac{q-1}{4}$  form a set of representatives for the conjugacy classes of  $\text{PSL}(2, q)$ . For  $1 \leq l \leq \frac{q-1}{4}$  and  $1 \leq m \leq \frac{q-1}{4}$ , one can see from [4, Theorem 38.1] that

$$|C_{\text{PSL}(2, q)}(1)| = |G|, \quad |C_{\text{PSL}(2, q)}(c)| = |C_{\text{PSL}(2, q)}(d)| = p,$$

$$|C_{\text{PSL}(2, q)}(a^l)| = \frac{q-1}{2}, \quad |C_{\text{PSL}(2, q)}(a^{\frac{q-1}{4}})| = q-1, \quad |C_{\text{PSL}(2, q)}(b^m)| = \frac{q+1}{2},$$

where  $p$  is the prime of which  $q$  is power. Now we count the elements which do not have  $r$ -th roots and will deduce the probability of having  $r$ -th roots.

Since  $\langle a \rangle \simeq C_r$ ,  $\langle a \rangle[r] \simeq \langle a \rangle$  and  $\langle a \rangle^r = 1$ , Proposition 2.2 (i) implies  $\text{Prob}_r(\langle a \rangle) = \frac{1}{r}$  so the elements not having  $r$ -th roots in  $\langle a \rangle$  are exactly

$$|\langle a \rangle - \langle a \rangle^r| = |\langle a \rangle| - |\langle a \rangle^r| = |\langle a \rangle| - 1 = r - 1 = \frac{q-1}{2} - 1 = \frac{q-3}{2}.$$

On the other hand, the (distinct) conjugates of  $\langle a \rangle$  have trivial intersection with  $\langle a \rangle$  so that the total number of elements of  $\text{PSL}(2, q)$  which do not have  $r$ -th roots is obtained by multiplying  $\frac{q-3}{2}$  by the number of conjugates of  $\langle a \rangle$ , which is  $|\text{PSL}(2, q) : N_{\text{PSL}(2, q)}(\langle a \rangle)|$ . This means that

$$\begin{aligned} |\text{PSL}(2, q)| - |\text{PSL}(2, q)^r| &= |\text{PSL}(2, q) - \text{PSL}(2, q)^r| \\ &= |\langle a \rangle - \langle a \rangle^r| \cdot |\text{PSL}(2, q) : N_{\text{PSL}(2, q)}(\langle a \rangle)| = \frac{q-3}{2} \cdot \frac{|\text{PSL}(2, q)|}{|N_{\text{PSL}(2, q)}(\langle a \rangle)|} \\ &= \frac{q-3}{2} \cdot \frac{|\text{PSL}(2, q)|}{q-1} \end{aligned}$$

and, dividing both sides by  $|\text{PSL}(2, q)|$ , we get

$$1 - \text{Prob}_r(\text{PSL}(2, q)) = \frac{q-3}{2} \cdot \frac{1}{q-1},$$

that is,

$$\text{Prob}_r(\text{PSL}(2, q)) = 1 - \frac{q-3}{2(q-1)} = \frac{q+1}{2(q-1)} = \frac{2(r+1)}{2(2r)} = \frac{r+1}{2r}.$$

□

We note that the case  $r = 2$ , which appears in the previous theorem, was found in [5, Proposition 3.1]. A consequence is the following.

**Corollary 3.2.** *Let  $q$  be a prime power. If  $q \equiv 1 \pmod{4}$ ,  $q$  is odd and  $r = \frac{q-1}{2} \geq 2$  is prime, then  $\lim_{r \rightarrow \infty} \text{Prob}_r(\text{PSL}(2, q)) = \frac{1}{2}$ .*

The computations for the projective special linear groups are important in order to get [3, Theorem 1.1] and to prove that the set

$$Z = \{\text{Prob}_2(G) \mid G \text{ is an arbitrary group}\}$$

is dense in  $[0, 1]$ . We are going to generalize for any prime  $r \geq 2$ , and we will not use projective special linear groups as done in [3, Theorem 1.1], but will assume a priori the existence of a certain group with a prescribed value of probability. This is justified by evidences of computational nature.

**Corollary 3.3.** *For any  $\epsilon \in \mathbb{R}$  with  $\epsilon > 0$  and given a prime  $r \geq 2$ , there exists an abelian group  $A$  such that  $0 < \text{Prob}_r(A) < \epsilon$ .*

*Proof.* Let  $k > 1$  be such that  $1/r^k < \epsilon$  and  $A$  be an elementary  $r$ -group of rank  $k$ . By Proposition 2.2 (ii), the result follows. □

A proof of Corollary 3.3 when  $r = 2$  can be found in [3]. Briefly, Corollary 3.3 shows that 0 is an accumulation point for the set  $X$  in Remark 2.1.

**Corollary 3.4.** *Assume that  $r \geq 2$  is a prime and  $S$  is a group such that  $\text{Prob}_r(S) = 1 - \frac{1}{|R|}$  for an elementary abelian  $r$ -Sylow subgroup  $R$  of  $S$ . Then for any  $\epsilon \in \mathbb{R}$  with  $\epsilon > 0$  we have  $1 - \epsilon < \text{Prob}_r(S) < 1$ .*

*Proof.* Since  $R$  is a Sylow  $r$ -subgroup of  $S$  which is elementary abelian of rank  $k$  for some  $k \geq 1$ , we have  $1/r^k < \epsilon$  and  $\text{Prob}_r(S) = 1 - \frac{1}{r^k} = \frac{r^k - 1}{r^k}$ . On the other hand,  $1 - \epsilon < \frac{r^k - 1}{r^k} < 1$ , therefore  $1 - \epsilon < \text{Prob}_r(S) < 1$ , as claimed.  $\square$

Corollary 3.4 when  $r = 2$  can be found in [3]. Also Corollary 3.3 is illustrating that 1 is an accumulation point for the set

$$T = \{\text{Prob}_r(G) \mid G \text{ is an arbitrary group}\},$$

where  $r \geq 2$  is a given prime.

**Theorem 3.5.** *Let  $r \geq 2$  be a prime and assume that there exists a group  $H$  such that  $\text{Prob}_r(H) = 1 - \frac{1}{|R|}$  for an elementary abelian  $r$ -Sylow subgroup  $R$  of  $H$ . Then the set  $T$  is dense in  $[0, 1]$ .*

*Proof.* By Corollaries 3.3, 3.4, there is no loss of generality in showing that, if  $0 < x < 1$ , then  $x$  is a limit point of  $T$ . There exists an integer  $m$  such that  $1/r < r^m x < 1$ . Note that  $(0, 1) = \bigcup_{m \geq 0} [1/r^{m+1}, 1/r^m]$ . Let  $y = r^m x$ . We can choose an integer  $n_1 \geq 1$  such that

$$(r^{n_1} - 1)/r^{n_1} \leq y \leq (r^{n_1+1} - 1)/r^{n_1+1},$$

noting that  $[1/r, 1) = \bigcup_{n \geq 1} [(r^n - 1)/r^n, (r^{n+1} - 1)/r^{n+1}]$ . Let  $s_1 = (r^{n_1} - 1)/r^{n_1}$  and  $r_1 = (r^{n_1+1} - 1)/r^{n_1+1}$ . Again we can choose an integer  $n_2 \geq 1$  such that

$$(r^{n_2} - 1)/r^{n_2} \leq y/r_1 \leq (r^{n_2+1} - 1)/r^{n_2+1},$$

noting that  $1/r \leq y/r_1 < 1$ . As before, let  $s_2 = (r^{n_2} - 1)/r^{n_2}$  and  $r_2 = (r^{n_2+1} - 1)/r^{n_2+1}$ . Iterating this process, there exist positive integers  $n_1, n_2, n_3, \dots$  and two sequences  $\{s_i\}$  and  $\{r_i\}$  such that  $s_i = (r^{n_i} - 1)/r^{n_i}$ ,  $r_i = (r^{n_i+1} - 1)/r^{n_i+1}$  and  $s_i \leq \frac{y}{r_1 r_2 \dots r_{i-1}} < r_i$  for all  $i \geq 1$ . Of course,  $0 < s_i < r_i < 1$  for all  $i \geq 1$ . We have  $n_i \leq n_{i+1}$  for all  $i \geq 1$ , since

$$s_i \leq \frac{y}{r_1 r_2 \dots r_{i-1}} < \frac{y}{r_1 r_2 \dots r_{i-1} r_i} < r_{i+1}.$$

Thus  $\{s_i\}$  is a monotonically increasing sequence, bounded by 1, and so convergent. Moreover,  $\{s_i\}$  has infinitely many distinct terms; otherwise  $\{s_i\}$ , and hence  $\{r_i\}$ , would be eventually constant, and so, for some  $j \geq 1$ , we would have

$$\frac{y}{r_1 r_2 \dots r_{j-1} r_j^{k-1}} < r_j$$

or  $r_1 r_2 \dots r_{j-1} r_j^k$  for  $k \geq 1$ . This is impossible, since  $y > 0$  and  $\lim_{k \rightarrow \infty} r_j^k = 0$ . Therefore,  $\{s_i\}$  converges to 1 (after omitting repeated terms), because it is a subsequence of  $\{(r^n - 1)/r^n\}$ . This allows us to note that the sequence  $\{a_i\}$  converges to 1, where  $a_i = y/r_1 r_2 \dots r_{i-1}$ . Consequently, the sequence  $\{b_i\}$  converges to  $y$ , where  $b_i = r_1 r_2 \dots r_{i-1}$ . Thus we have

$$\lim_{k \rightarrow \infty} \frac{r_1 r_2 \dots r_{i-1}}{r^m} = \frac{y}{r^m} = x.$$

For each  $i \geq 1$  we consider the group  $G^{(i)} = G_0 \times G_1 \times \dots \times G_{i-1}$ , where  $G_0 = C_r^m$  and  $G_k$  is a sequence of groups isomorphic for each  $k$  to the group  $H$ , introduced

in the assumptions. Propositions 2.2 and 2.6 imply

$$\text{Prob}_r(G^{(i)}) = \text{Prob}_r(G_0) \text{Prob}_r(G_1) \dots \text{Prob}_r(G_{i-1}) = \frac{1}{r^m} r_1 r_2 \dots r_{i-1}.$$

We have  $\lim_{i \rightarrow \infty} \text{Prob}_r(G^{(i)}) = x$  and the result follows.  $\square$

## REFERENCES

- [1] J. Blum, Enumeration of the square permutations in  $S_n$ , *J. Comb. Theory Ser. A* **17** (1974), 156–161.
- [2] M. Bóna, A. McLennan and D. White, Permutations with roots, *Random structures and algorithms* **17** (2) (2000), 157–167.
- [3] A.K. Das, On group elements having square roots, *Bull. Iranian Math. Soc.* **31** (2005), 33–36.
- [4] L. Dornhoff, *Group Representation Theory*, Part A, Marcel Dekker, New York, 1971.
- [5] M.S. Lucido and M.R. Pournaki, Elements with square roots in finite groups, *Algebra Colloq.* **12** (2005), 677–690.
- [6] M.S. Lucido and M.R. Pournaki, Probability that an element of a finite group has a square root, *Colloq. Math.* **112** (2008), 147–155.
- [7] N. Pouyanne, On the number of permutations admitting an  $m$ -th root, *Electr. J. Comb.* **9** (2002), 12 pp. (electronic).
- [8] F.G. Russo, Elements with square roots in compact groups, *Asian Eur. J. Math.* **3** (2010), 495–500.

DEPARTMENT OF MATHEMATICS, ISLAMIC AZAD UNIVERSITY, MASHHAD-BRANCH, 91756, MASHHAD, IRAN

*E-mail address:* `elahehkhamsheh@gmail.com`

DEPARTMENT OF MATHEMATICS, KHAYYAM HIGHER EDUCATION INSTITUTE, AND CENTRE OF EXCELLENCE IN ANALYSIS AND ALGEBRAIC STRUCTURE OF FERDOWSI UNIVERSITY OF MASHHAD, MASHHAD, IRAN

*E-mail address:* `mrrm5@yahoo.ca`

DIEETCAM, UNIVERSITY OF PALERMO, VIALE DELLE SCIENZE, 90128, PALERMO, ITALY, AND, DEPARTMENT OF MATHEMATICS, UNIVERSITI TEKNOLOGI MALAYSIA, 81310, SKUDAI, JOHOR BAHRU, MALAYSIA

*E-mail address:* `francescog.russo@yahoo.com`

DEPARTMENT OF MATHEMATICS, ISLAMIC AZAD UNIVERSITY, MASHHAD-BRANCH, 91756, MASHHAD, IRAN

*E-mail address:* `saeedi@mshdiau.ac.ir`